DISABLING PROHIBITED CONTENT AND IDENTIFYING REPEAT OFFENDERS IN SERVICE PROVIDER STORAGE SYSTEMS

BACKGROUND

Computer users increasingly share data through storage systems hosted by service providers on computer networks such as the internet. Service providers, however, may be required to address situations in which users share content for which distribution is prohibited, such as unlicensed copyrighted works or trademarked goods, which are brought to the attention of the service provider by a third party. Other types of prohibited content include, but are not limited to, other intellectual property or defamatory content in some jurisdictions.

There are a variety of ways in which service providers determine that prohibited content exists on a system. However, even if such content is identified, a question that remains is what to do about it.

SUMMARY

This Summary introduces selected concepts in simplified form that are further described below in the Detailed Description. This Summary is intended neither to identify key or essential features of the claimed subject matter, nor to limit the scope of the claimed subject matter.

When objects are shared by one user with another user, prohibited content, if identified as such, can be blocked from being shared, while the remainder of the shared objects can be accessed by the other user. Incidents that occur related to such prohibit content, such as marking the content in response to a third party notification that such content is prohibited, are stored in a history for a user. This history is processed to determine if a user is a repeat offender. Various account privileges from the service provider can be affected when a user becomes a repeat offender, such as termination of the account, prevention of sharing of files through the account, and the like.

In one example implementation, metadata for each data file can include a prohibited content flag indicating whether the file has been marked as containing prohibited content. Functions that allow sharing of content are implemented so as prevent sharing of prohibited content with another user, while allowing other content to be shared. If a group of files or objects is shared, then the presence of the prohibited content in one object in the group results in that prohibited content not being shared, but the remaining files or objects are still shared.

In one example implementation, metadata associated with each user includes an incident history, including a date and information about one or more files that were deemed to contain prohibited content. The information can include a file name or other identifier for an object, a hash of contents of the object, or other indication of the object. The information also can indicate the nature of the incident, such as a copyright violation, and the like. When an incident occurs with respect to a user, and that user's content is marked as prohibited, the incident history is updated. The incident history can be processed after an incident is added to determine if rules for changing the access privileges of the user are triggered. For example, if a number of incidents in a given time period occur, the access privileges of the user can be changed, for example, to prevent sharing files with other users.

A graphical user interface for accessing the storage system, whether by providers or recipients of shared content, can selectively render information about objects with prohibited content. For example, the interface can indicate the presence of an object, but access to prohibited content in that object can remain limited. In one implementation, the interface can present information indicating that access to the object is blocked due to its inclusion of prohibited content.

In an implementation in a file system, other file system operations can be implemented to allow access to parts of the file or data about the file, but the prohibited content is not made available. For example, in one implementation a file includes multiple file streams, including at least a metadata stream and a data stream. If a file contains prohibited content in the data stream, then access to the data stream is prevented; however, access to the metadata stream can be enabled. Metadata that is derivative of the prohibited content also can be removed, not generated or made not accessible. For example, for image files, a reduced image, representative of the image in the file, can be either removed, not generated, or made not accessible. Because the file is stored in a shared storage system, what data is made available about the file, and how it is stored, can also be function of both the prohibited content flag, the access privileges of the user that created the file, and the identity or role of the user accessing the file, using access control information for the file.

Such a prohibited content flag on a file object can be used in combination with one or more other flags that indicate that access to a file object, such as sharing of a file object, is blocked. For example, objectionable content may be marked using a restricted content flag. Such a file object also can be marked as including prohibited content. Sharing of content from such a file object can be blocked if either or both flags are set for a file object, while changes to a user's access privileges may be limited to incidents related to marking a file object as containing prohibited content.

In the following description, reference is made to the accompanying drawings which form a part hereof, and in which are shown, by way of illustration, specific example implementations of this technique. It is understood that other embodiments may be utilized and structural changes may be made without departing from the scope of the disclosure.

DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram of an example shared storage system from a service provider.

FIG. **2** is a data flow diagram illustrating an example implementation of access restrictions

FIG. **3** is a flow chart of an example implementation of uploading content to the storage system.

FIG. **4** is a flow chart of an example implementation of accessing content on the storage system.

FIG. **5** is a flow chart of an example implementation of sharing content on the storage system.

FIG. **6** is a flow chart of an example implementation of changing access privileges of a user based on an incident history.

FIG. **7** is a block diagram of an example computer with which components of such a system can be implemented.

DETAILED DESCRIPTION

The following section provides an example operating environment in which a shared storage system can be implemented. This example is provided in the context of an